

WE CLAIM:

1. A computer program product comprising a computer program operable to control a computer to generate audit data indicative of a request to execute a computer program,
5 said computer program comprising:

(i) computer virus scanner logic operable to receive a computer virus scan request, said computer virus scan request including data identifying a computer file to be scanned for computer viruses; and

(ii) audit data generator logic triggered by said computer virus scanner logic,
10 and responsive to said data identifying said computer file to be scanned, to identify a request to execute a computer program and, in response to identification of said request to execute said computer program, to generate audit data identifying said computer program.

2. A computer program product as claimed in claim 1, wherein a file access request to an operating system triggers generation of said computer virus scan request.

3. A computer program product as claimed in claim 1, wherein said audit data generator logic is responsive to data identifying one or more banned computer programs
20 to identify a request to execute a banned computer program.

4. A computer program product as claimed in claim 3, wherein, if a request to execute a banned computer program is identified, then one or more banned program actions are triggered, said banned program actions including one or more of:

- 25 (i) said banned computer program is deleted;
(ii) said banned computer program is disabled;
(iii) said banned program is encrypted and replaced by a stub program; and
(iv) an alert indicating detection of said banned computer program is issued.

30 5. A computer program product as claimed in claim 3, wherein said data identifying one or more banned computer programs is a permitted computer program list with any

computer program not included within said permitted computer program list being a banned computer program.

6. A computer program product as claimed in claim 1, further comprising concurrent
5 usage logic operable to perform a concurrent usage check to identify a request to execute a computer program that would result in said computer program concurrently executing upon more than a predetermined number of computers upon a computer network.

7. A computer program product as claimed in claim 6, wherein, if said concurrent
10 usage check indicates that said request to execute said computer program would result in more than said predetermined number of computers upon said computer network concurrently executing said computer program, then said request to execute said computer program is denied.

8. A computer program product as claimed in claim 7, wherein a user message is
15 displayed when execution of said computer program is prevented.

9. A computer program product as claimed in claim 6, wherein said predetermined
20 number varies with time.

10. A computer program product as claimed in claim 9, wherein at certain times said
predetermined number is zero.

11. A computer program product as claimed in claim 1, wherein said audit data
25 generator logic calculates a checksum value from said computer file, said checksum value being used in identification of said computer file as a particular computer program.

12. A computer program product as claimed in claim 11, wherein said audit data
30 generator logic stores said calculated checksum value and uses said stored calculated checksum values instead of recalculating said checksum value when said computer file

subject to a subsequent access without any intervening change having been made to said computer file.

13. A computer program product as claimed in claim 1, wherein said audit data generator logic is responsive to a non-user specified database of data indicative of particular computer programs.

14. A computer program product as claimed in claim 1, wherein said audit data generator logic is responsive to a user specified database of data indicative of particular computer programs.

15. A computer program product as claimed in claim 1, wherein said computer virus scan request results from an on-access scan.

16. A computer program product as claimed in claim 1, wherein said computer virus scan request results from an on-demand scan.

17. A computer program product as claimed in claim 1, wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer.

18. A computer program product as claimed in claim 17, wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network.

19. A method of generating audit data indicative of a request to execute a computer program, said method comprising the steps of:

(i) receiving a computer virus scan request within a computer virus scanner, said computer virus scan request including data identifying a computer file to be scanned for computer viruses;

(ii) triggering operation of an audit data generator using said computer virus scanner, said audit data generator being responsive to said data identifying said computer file to be scanned to identify a request to execute a computer program; and

(iii) in response to identification of said request to execute said computer program, generating audit data identifying said computer program.

20. A method as claimed in claim 19, wherein a file access request to an operating system triggers generation of said computer virus scan request.

21. A method as claimed in claim 19, wherein said audit data generator is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program.

22. A method as claimed in claim 21, wherein, if a request to execute a banned computer program is identified, then one or more banned program actions are triggered, said banned program actions including one or more of:

- (i) said banned computer program is deleted;
- (ii) said banned computer program is disabled;
- (iii) said banned program is encrypted and replaced by a stub program; and
- (iv) an alert indicating detection of said banned computer program is issued.

23. A method as claimed in claim 21, wherein said data identifying one or more banned computer programs is a permitted computer program list with any computer program not included within said permitted computer program list being a banned computer program.

24. A method as claimed in claim 19, further comprising performing a concurrent usage check to identify a request to execute a computer program that would result in said computer program concurrently executing upon more than a predetermined number of computers upon a computer network.

25. A method as claimed in claim 24, wherein, if said concurrent usage check indicates that said request to execute said computer program would result in more than said predetermined number of computers upon said computer network concurrently executing said computer program, then said request to execute said computer program is denied.

26. A method as claimed in claim 25, wherein a user message is displayed when execution of said computer program is prevented.

27. A method as claimed in claim 24, wherein said predetermined number varies with time.

28. A method as claimed in claim 27, wherein at certain times said predetermined number is zero.

29. A method as claimed in claim 19, wherein said audit data generator calculates a checksum value from said computer file, said checksum value being used in identification of said computer file as a particular computer program.

30. A method as claimed in claim 29, wherein said audit data generator stores said calculated checksum value and uses said stored calculated checksum values instead of recalculating said checksum value when said computer file subject to a subsequent access without any intervening change having been made to said computer file.

31. A method as claimed in claim 19, wherein said audit data generator is responsive to a non-user specified database of data indicative of particular computer programs.

32. A method as claimed in claim 19, wherein said audit data generator is responsive to a user specified database of data indicative of particular computer programs.

33. A method as claimed in claim 19, wherein said computer virus scan request results from an on-access scan.

34. A method as claimed in claim 19, wherein said computer virus scan request results from an on-demand scan.

35. A method as claimed in claim 19, wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer.

36. A method as claimed in claim 35, wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network.

37. Apparatus for generating audit data indicative of a request to execute a computer program, said apparatus comprising:

(i) a computer virus scanner operable to receive a computer virus scan request, said computer virus scan request including data identifying a computer file to be scanned for computer viruses; and

(ii) an audit data generator triggered by said computer virus scanner logic, and responsive to said data identifying said computer file to be scanned, to identify a request to execute a computer program and, in response to identification of said request to execute said computer program, to generate audit data identifying said computer program.

38. Apparatus as claimed in claim 37, wherein a file access request to an operating system triggers generation of said computer virus scan request.

39. Apparatus as claimed in claim 37, wherein said audit data generator is responsive to data identifying one or more banned computer programs to identify a request to execute a banned computer program.

40. Apparatus as claimed in claim 39, wherein, if a request to execute a banned computer program is identified, then one or more banned program actions are triggered, said banned program actions including one or more of:

- (i) said banned computer program is deleted;
- (ii) said banned computer program is disabled;
- (iii) said banned program is encrypted and replaced by a stub program; and
- (iv) an alert indicating detection of said banned computer program is issued.

41. Apparatus as claimed in claim 39, wherein said data identifying one or more banned computer programs is a permitted computer program list with any computer program not included within said permitted computer program list being a banned computer program.

42. Apparatus as claimed in claim 37, further comprising a concurrent usage monitor operable to perform a concurrent usage check to identify a request to execute a computer program that would result in said computer program concurrently executing upon more than a predetermined number of computers upon a computer network.

43. Apparatus as claimed in claim 42, wherein, if said concurrent usage check indicates that said request to execute said computer program would result in more than said predetermined number of computers upon said computer network concurrently executing said computer program, then said request to execute said computer program is denied.

44. Apparatus as claimed in claim 43, wherein a user message is displayed when execution of said computer program is prevented.

45. Apparatus as claimed in claim 42, wherein said predetermined number varies with time.

46. Apparatus as claimed in claim 45, wherein at certain times said predetermined number is zero.

47. Apparatus as claimed in claim 37, wherein said audit data generator calculates a checksum value from said computer file, said checksum value being used in identification of said computer file as a particular computer program.

48. Apparatus as claimed in claim 47, wherein said audit data generator stores said calculated checksum value and uses said stored calculated checksum values instead of recalculating said checksum value when said computer file subject to a subsequent access without any intervening change having been made to said computer file.

49. Apparatus as claimed in claim 37, wherein said audit data generator is responsive to a non-user specified database of data indicative of particular computer programs.

50. Apparatus as claimed in claim 37, wherein said audit data generator is responsive to a user specified database of data indicative of particular computer programs.

51. Apparatus as claimed in claim 37, wherein said computer virus scan request results from an on-access scan.

52. Apparatus as claimed in claim 37, wherein said computer virus scan request results from an on-demand scan.

53. Apparatus as claimed in claim 37, wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer.

54. Apparatus as claimed in claim 53, wherein said remote computer generates a consolidated audit report for a plurality of computers upon said computer network.